Product Name	Confidentiality level
mToken CryptoID	
Product version	
V3.0	

mToken CryptoID on Linux/Mac OS

Century Longmai Technology Co., Ltd.

Revision Record

Date	Revision Version	Sec No.	Change Description	Author
2015/12/02	V1.0		Initial Version	Longmai ITD

Contents

1. Introduction

mToken CryptoID is smartcard USB token compliant with both standards PC/SC and CCID. The mToken CryptoID provides pkcs11 middleware for Linux and Mac OS, which could be used by the applications, like firefox, thunderbird, etc.

This document describes how to use it from these applications, it's same on both Linux and Mac OS.

The PKCS11 module could be found from the pkcs11 folder of the SDK. You can find the module file by different OS.

2. Add access rules for mToken CryptoID on Linux

The USB device is not allowed to access by non-root user until adding access rules into the udev sub system on linux.

Please put the “90-mtoken.rules” into /etc/udev/rules.d with root account and re-plugin the token, then you can access it with the pkcs11 from applications.

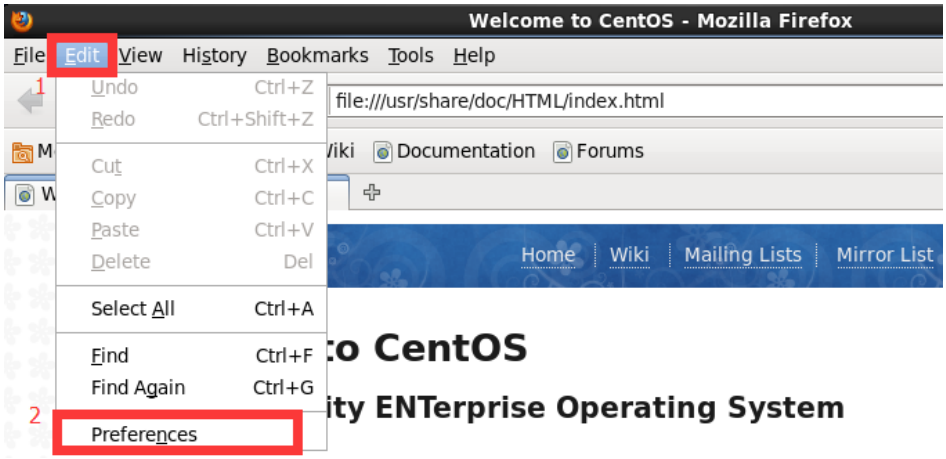
There is no need to do so for MAC OS system.

3. Firefox Usage Guide

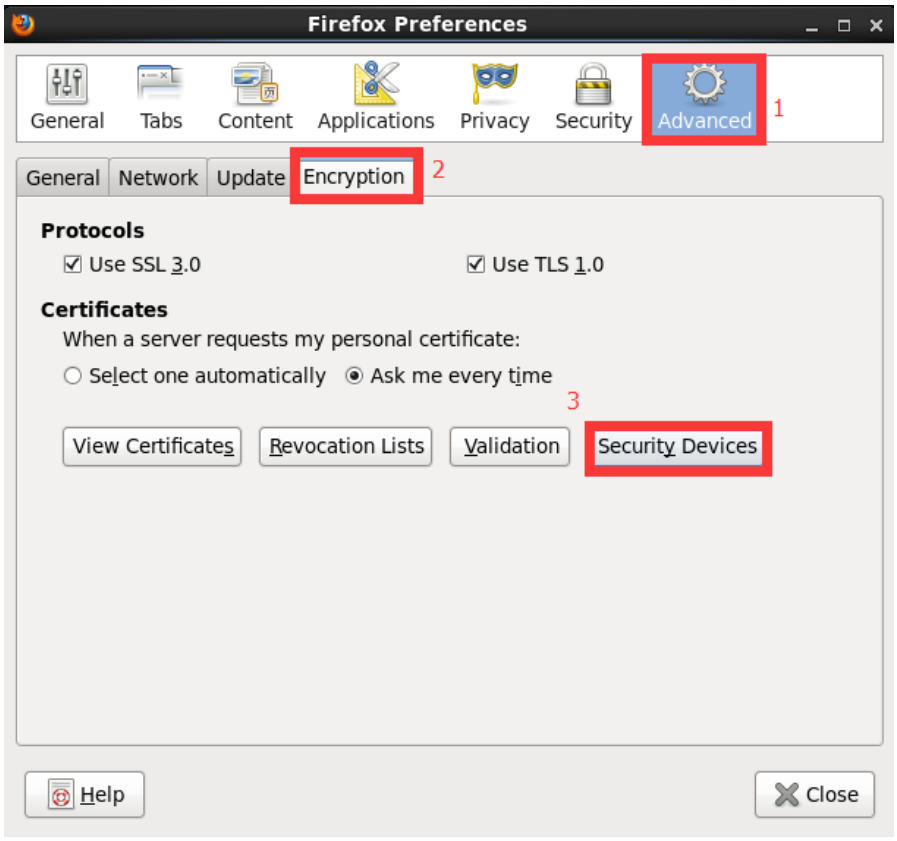
To integrate Firefox browser with mToken CryptoID device, you need to first perform some configurations.

Start Firefox, and perform the following operations step by step:

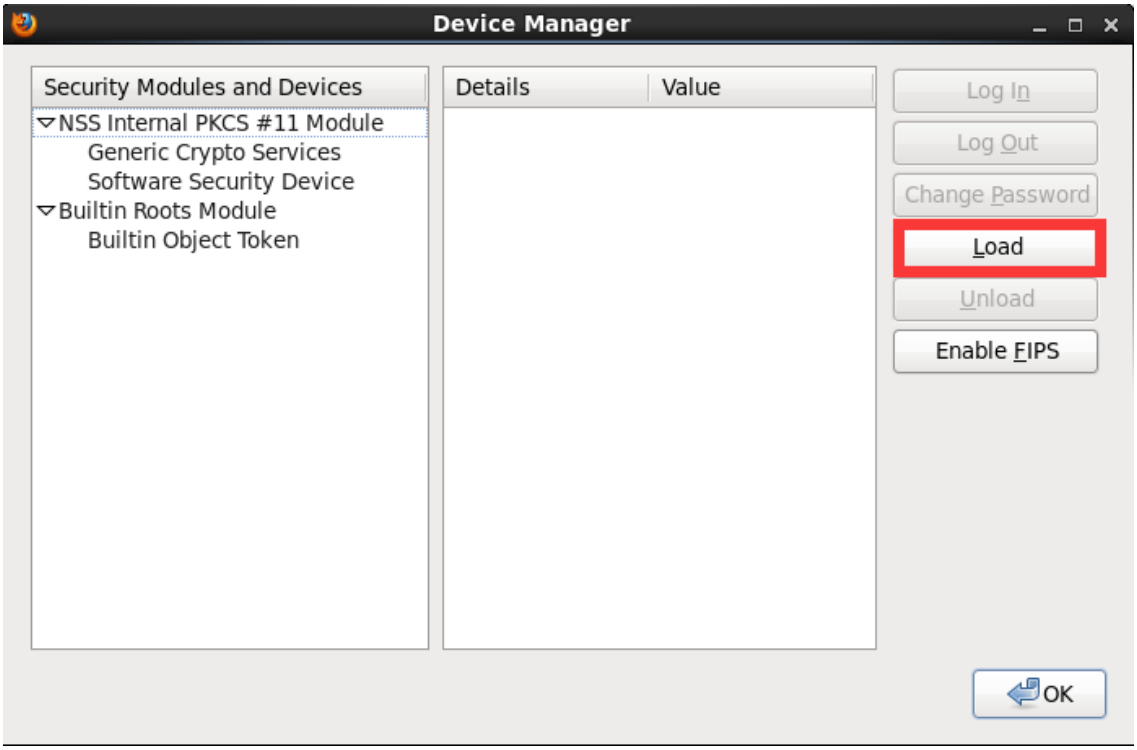
1. Start Firefox, and then select **Edit→Preferences**.



2. The **Firefox Preferences** bullet box will pop up, select **Advanced →Encryption → Security Devices**.

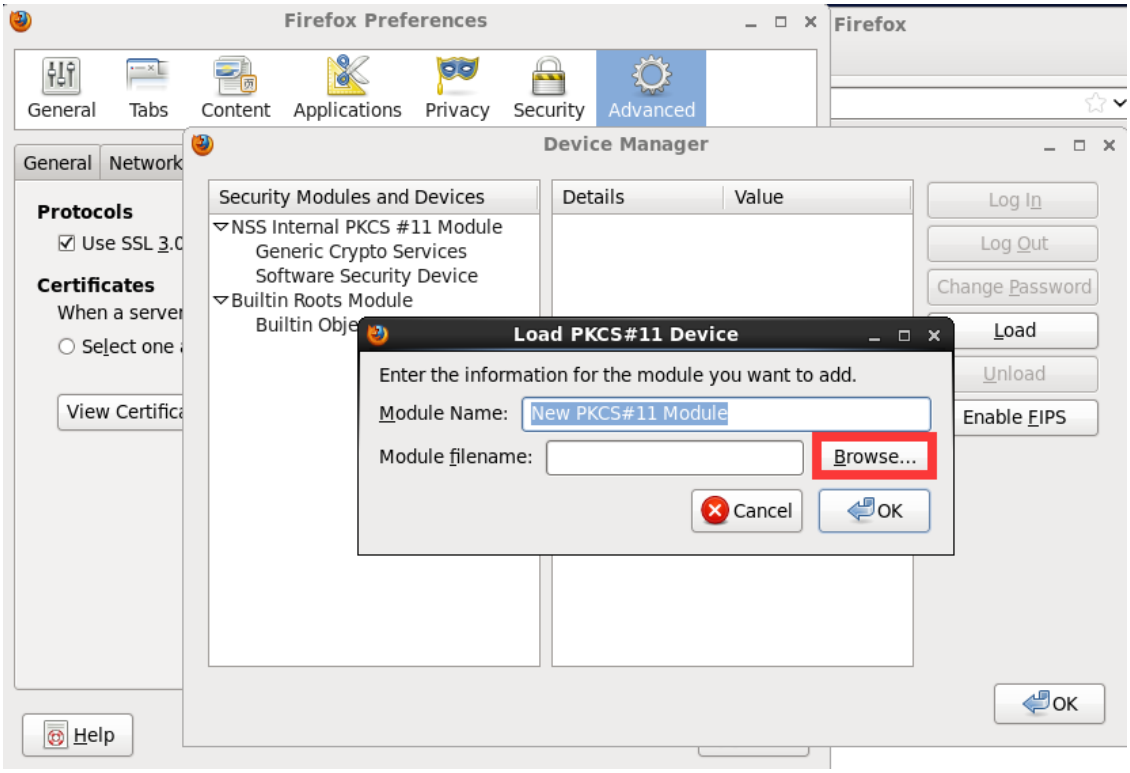


3. Click **Security Devices**, the Device Manager appears, then click **Load** to load PKCS#11 device.

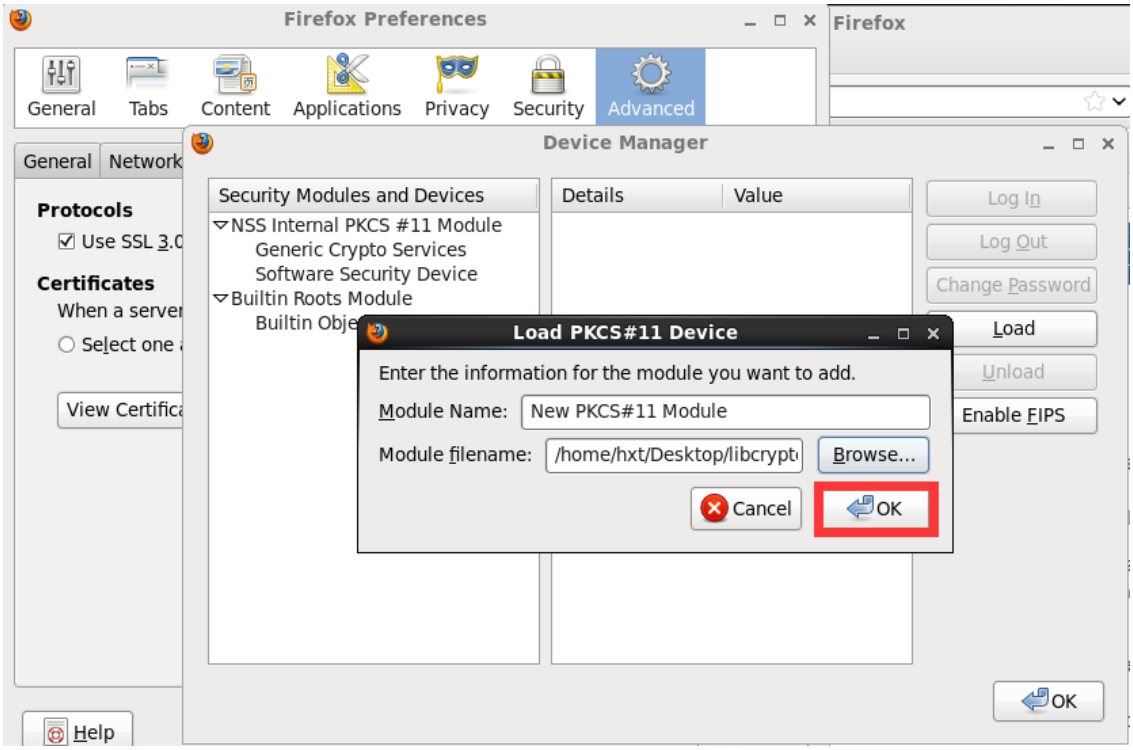


4. Specify a name and a path for the security module.

   Path: /usr/lib/cryptoide_pkcs11.so, for example.



Select the PKCS11 module file and click **OK** to load.

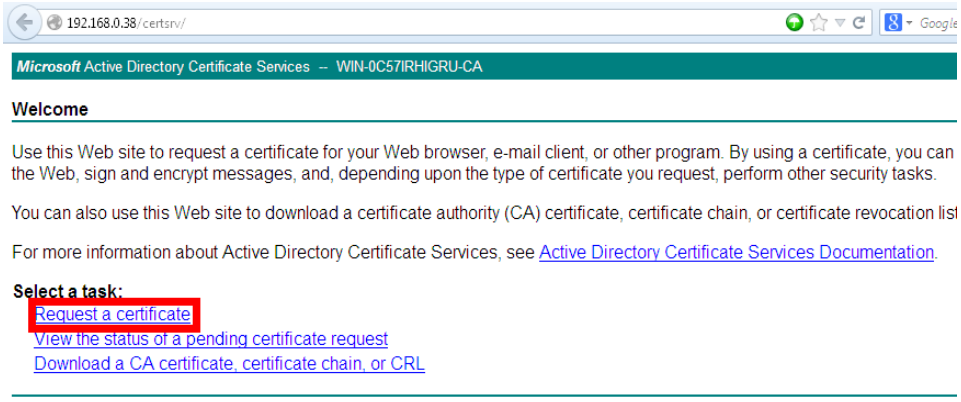


5. The module is displayed on the left panel. The shown name is what you typed above. Now, you have already integrated Firefox with mToken CryptoID successfully, you can try to login and logout the mToken CryptoID device.

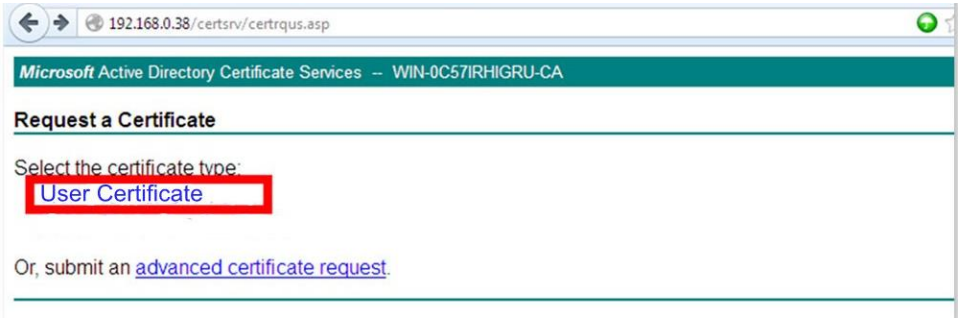
3.1 Using PKCS#11 Interface to request a Digital Certificate

The process of requesting a certificate using the PKCS#11 interface through the Firefox browser on Linux platform is described below:

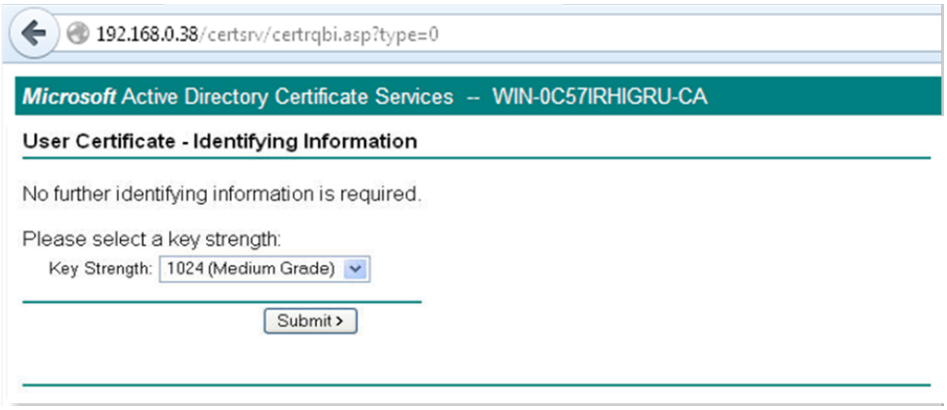
1. Make sure you have connected and initialized mToken CryptoID device on your computer. Start Firefox and open your CA's Webpage. Then, select **Request a certificate**.



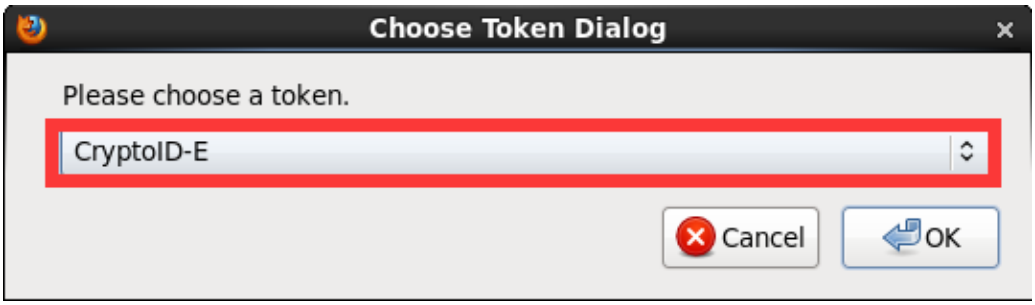
2. Click Next to continue, the certificate type page appears, Select **User Certificate**.



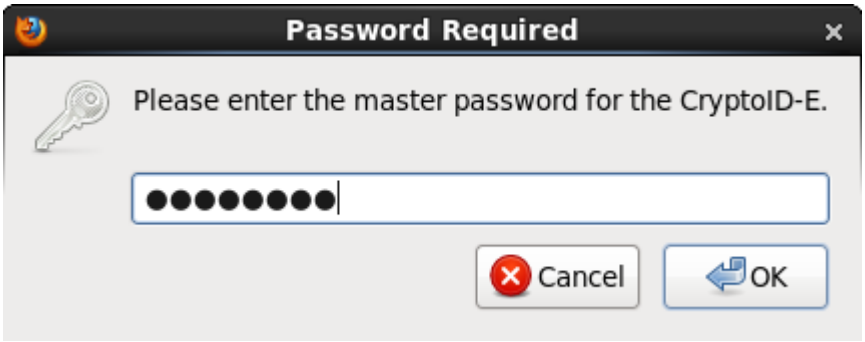
3. Click Next to continue, the key length page appears. Select an appropriate length from the drop-down list.



4. Click **Submit**, the token selection page appears. Select the correct device and click **OK**.



5. Type the correct PIN in the dialog box that pops up.



Note: The PIN input box will not be displayed if you have logged in at the final step described in section 1.1.

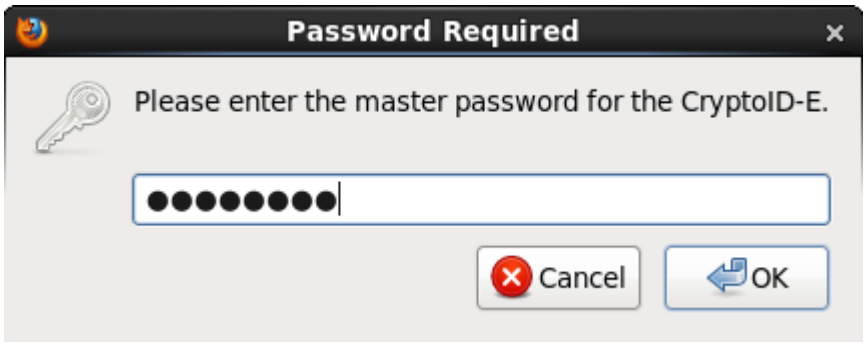
6. Click **OK**; a key pair will be generated:

7. After generating the key pair, the key information and personal information are sent to the CA. The CA will issue a certificate based on this information provided. Once the certificate has been issued successfully, the following page will appear:

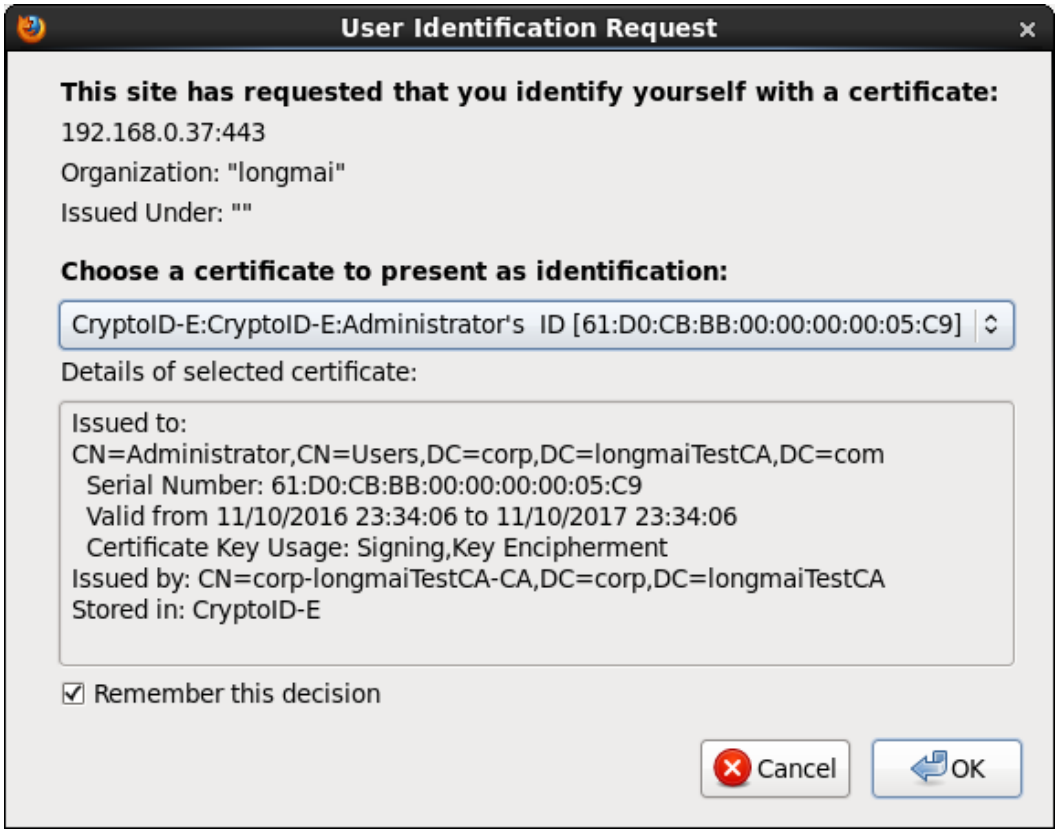
8. Click **Install this certificate** link on above page, Firefox will install this certificate to mToken. At this step, you have completed the certificate request process.

3.2 Using PKCS#11 Interface to access SSL encrypted Website

1. Make sure you have connected mToken CryptoID device (containing certificate) to your computer. Then start Firefox, accessing the SSL encrypted Website with the HTTPS protocol.
2. If everything works fine, Firefox will alert PIN boxes of all connected security devices one after the other. In this case, only the mToken device is connecting to the computer:



3. Type the correct PIN and click **OK**, Firefox will call PKCS#11 Interface. The key and certificate information will be loaded from the device, and a list of all available certificates will be displayed for user selection.



Note: If you have specified **Select Automatically** in Client Certificate Selection area as

shown in 1.1, the certificate will be selected automatically and the certificate selection dialog box as shown above will not be displayed. The dialog box appears only if you have specified **Ask Every Time**.

4. Select an appropriate certificate and click **OK**. After a series of information exchange and authentication, the request page will be displayed (the following is an example site):

4. Thunderbird Usage Guide

4.1 Using PKCS#11 Interface to send/receive Signed, Encrypted messages

This section describes how to obtain a secure mail certificate; send/receive signed, encrypted messages using the PKCS#11 interface in Thunderbird on Linux platform. Before configuring Thunderbird for dispatching signed, encrypted messages, make sure that you are able to connect to the email server and communicate using Thunderbird normally. First of all, you must obtain a certificate for mail security.

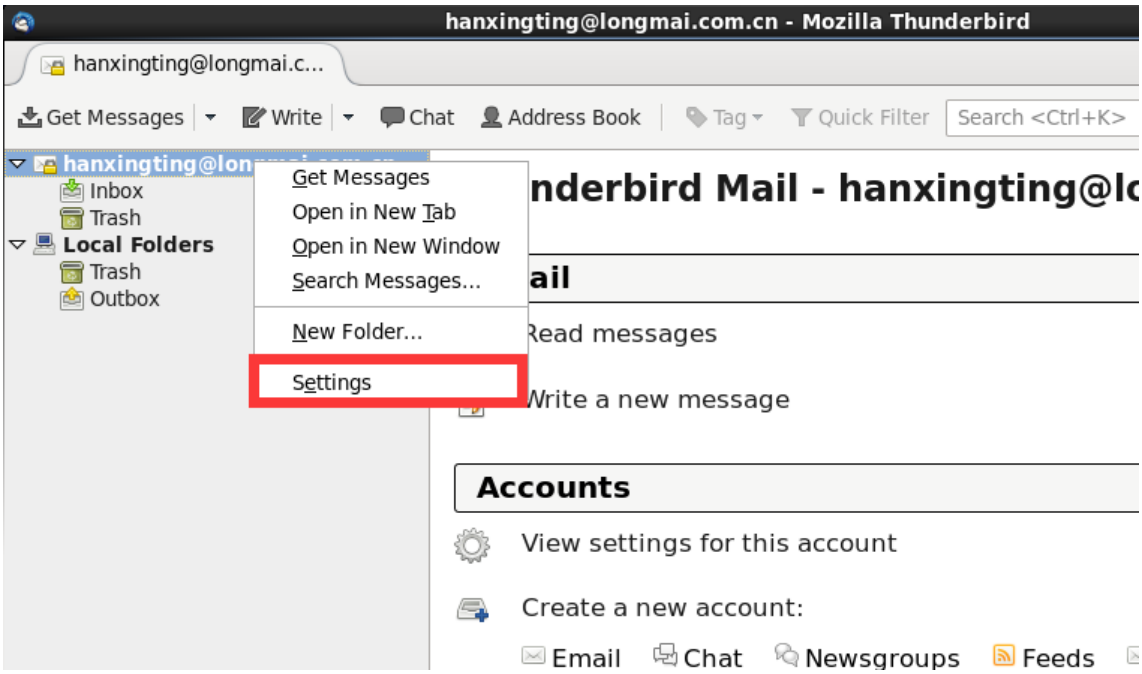
4.1.1 Obtaining a Secure Mail Certificate

You can obtain certificate as described in section 1.2, the detail request method have something to do with the configuration of CA Server. The certificate must have an email property. You can configure the Email Account in Thunderbird when you get a digital certificate, then the email account has ability to do with security messages.

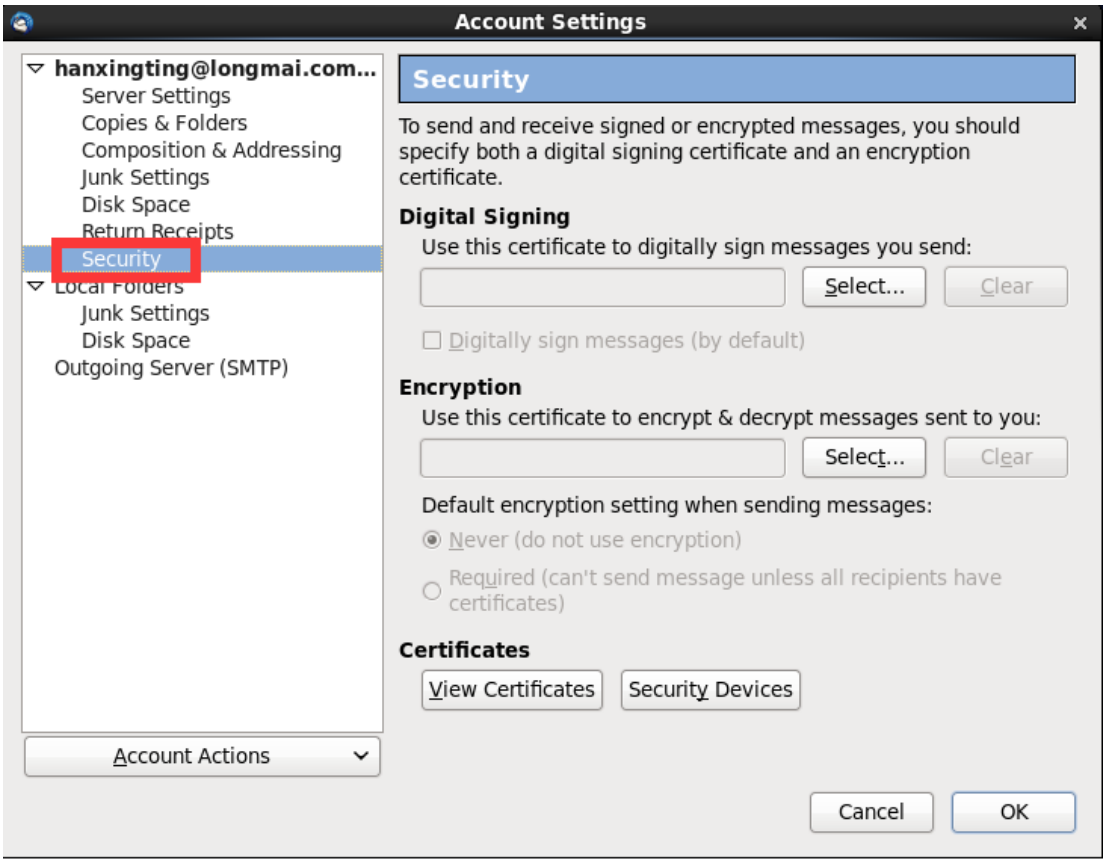
4.1.2 Integrate mToken with Thunderbird

To integrate mToken with Thunderbird, perform the following operations:

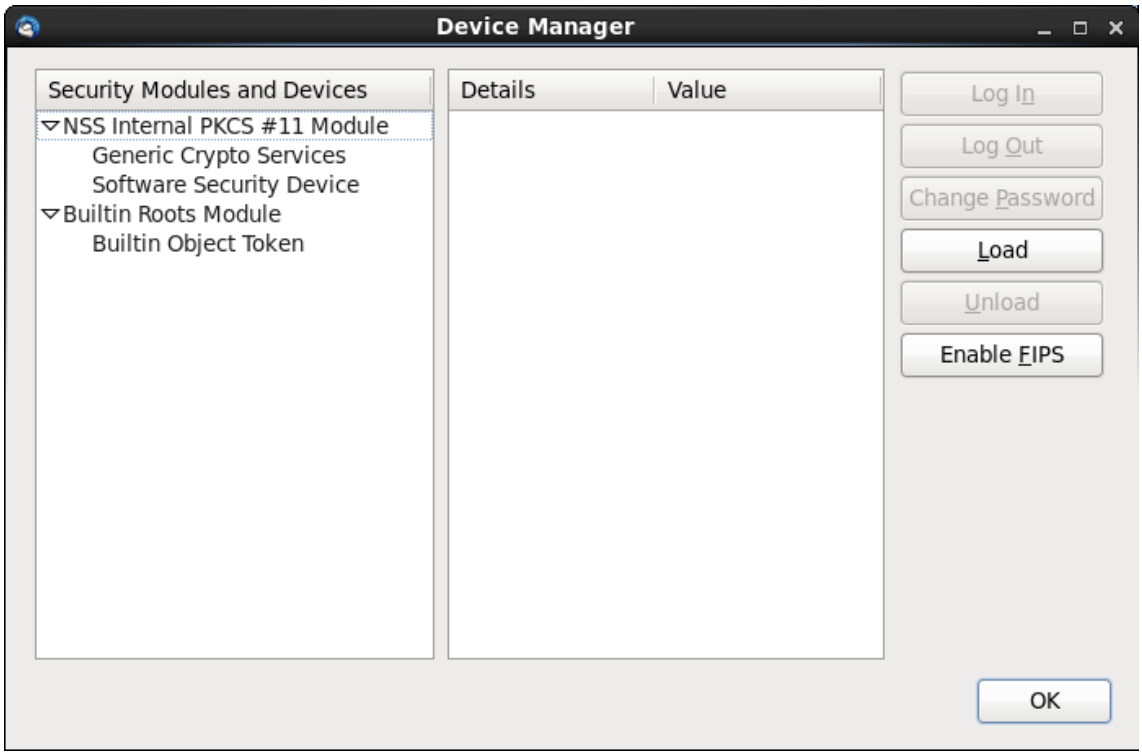
1. Start Thunderbird, select the account and right click **Settings**.



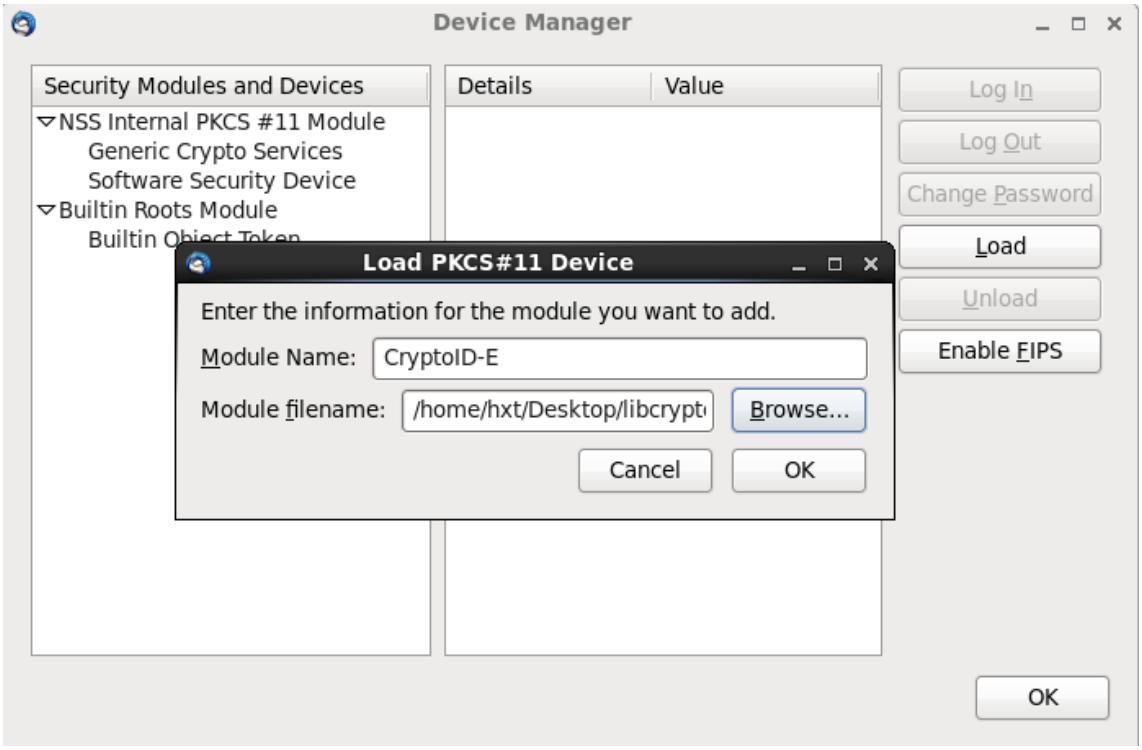
2. The **Account Setting** dialog box appears, select **Security** on the left tree. The Security configuration page appears on the right side of the window.



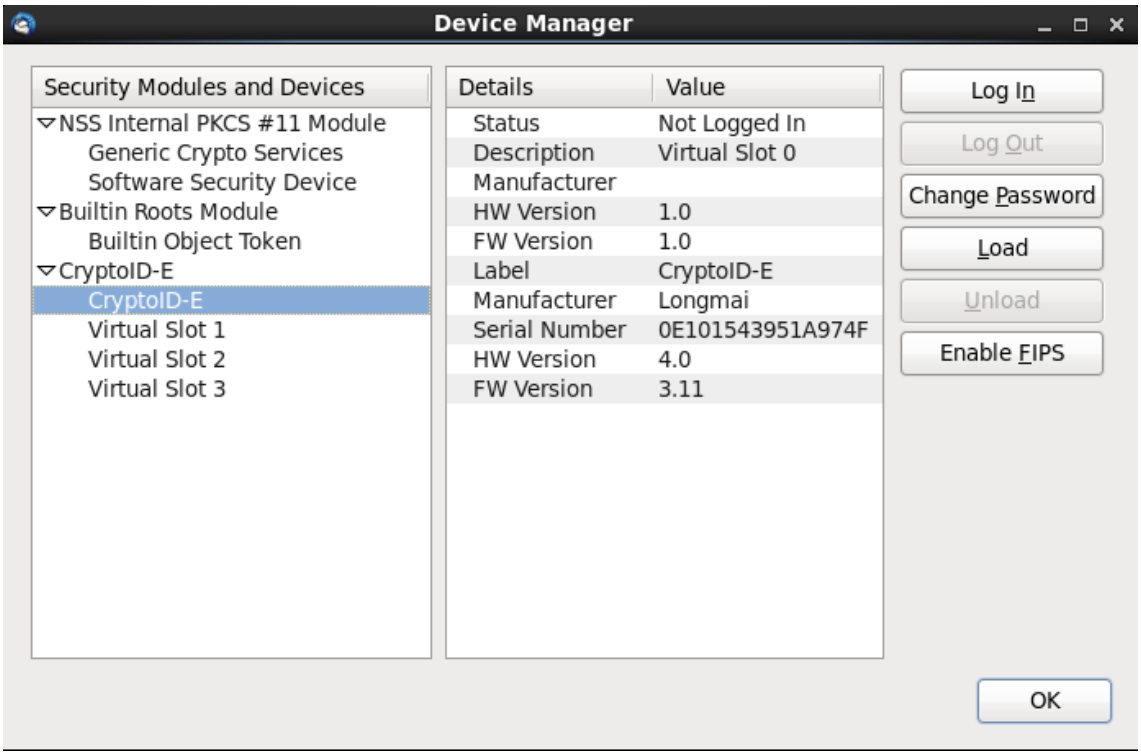
3. Click **Security Devices**, the Device Manager window will pop up.



4. Click **Load**, type module name and click **Browse** to select PKCS#11 module from system.



5. Click **OK**, the loaded the PKCS#11 module will show in the list.



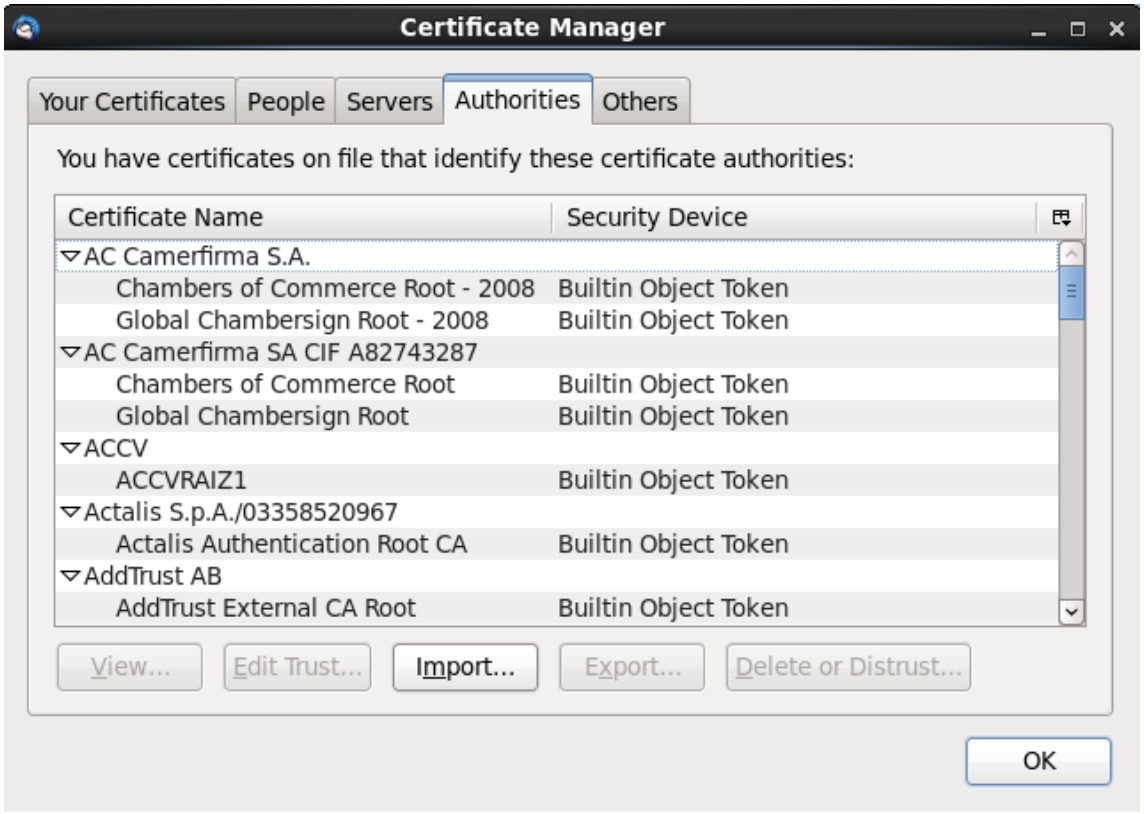
6. At this point, the mToken and Thunderbird have been integrated successfully; you can Log In, Log Out, Change Password and Unload mToken device.

4.1.3 Configuring E-mail Account Security in Thunderbird

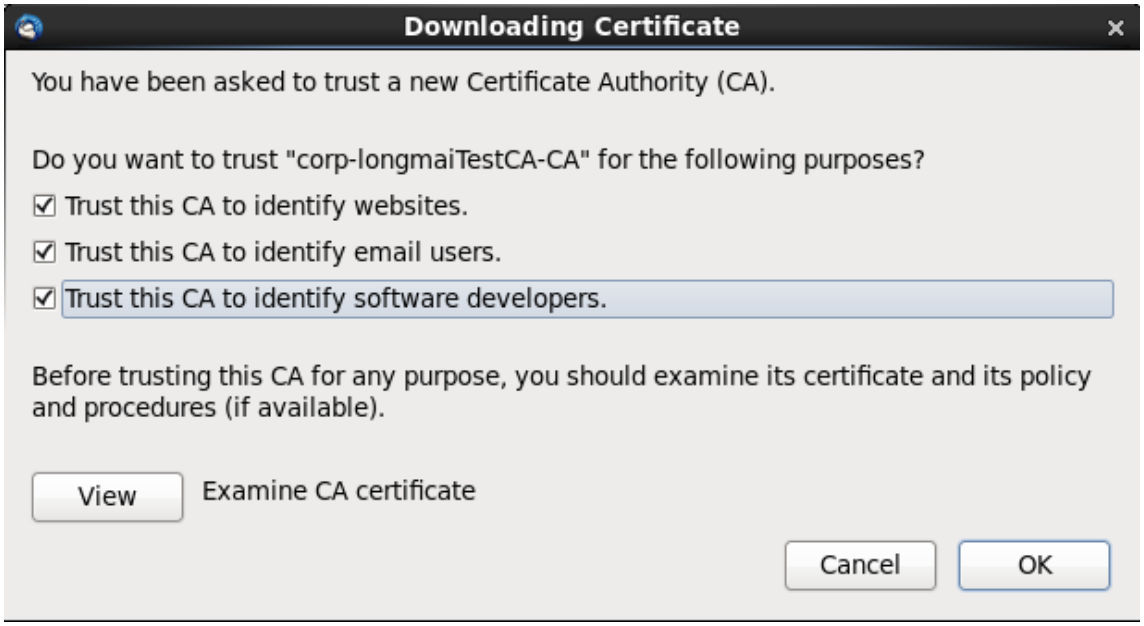
To use user certificate, we should import root certificate so that we can use its public key.

To configure the security of Email Account, perform the following operations:

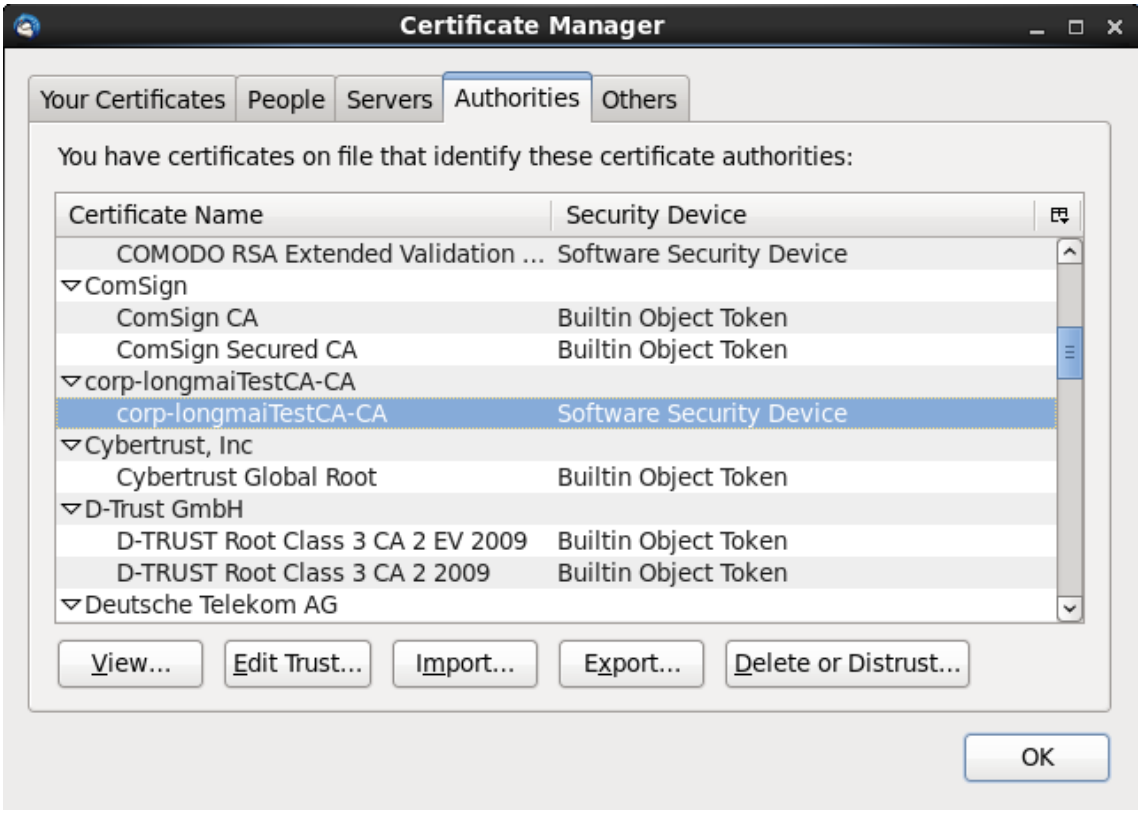
1. Click **Settings** →**Security** →**View Certificates** →**Authorities.** Here you can see all trusted certificate authorities.



2. Click **Import**, select root certificate.
3. Select purpose, here I select trust all.

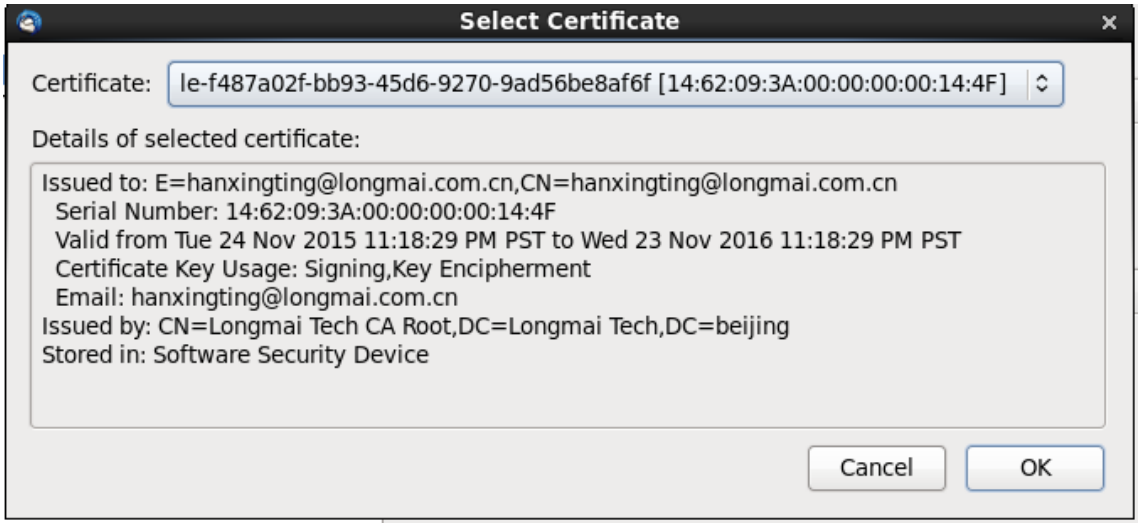


4. Click **OK**, the root certificate has been added in Authorities.

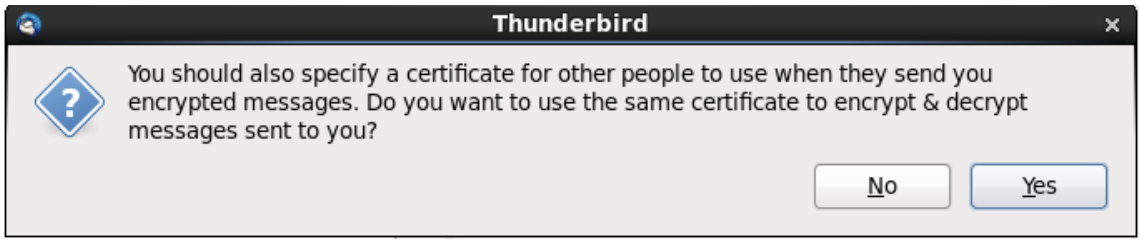


5. Ok, now close the window, back to Account Settings window.

6. Click **Select** in Digital Signing area. The signing certificates for account in the device are listed in a dialog box.



7. Select a mail certificate and click **OK**. The certificate will be filled out in the field before the button in Digital Signing area. At the same time, another dialog box is displayed, asking you to specify a certificate for others who will send you encrypted messages.



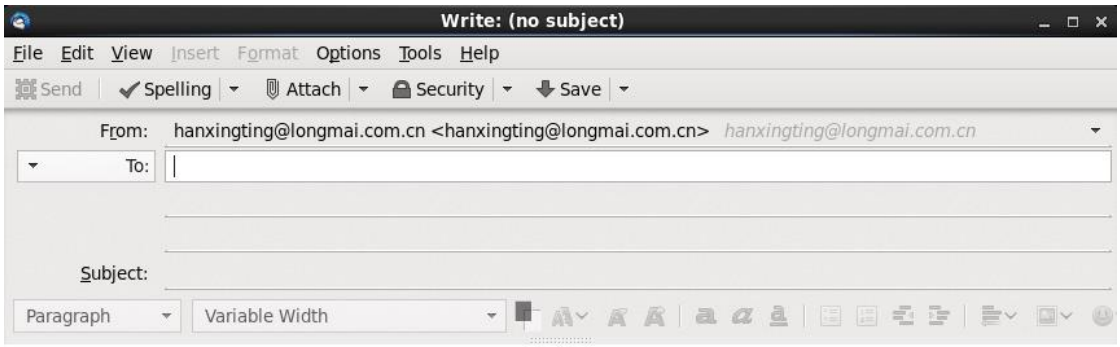
8. Click **Yes**, the digital certificate will be used as encrypt certificate automatically.

You can select **Digital sign messages** to use it sign as default, you can also select **Required (can't send message unless all recipients have certificates).** You can also use below methods to sign or encrypt messages.

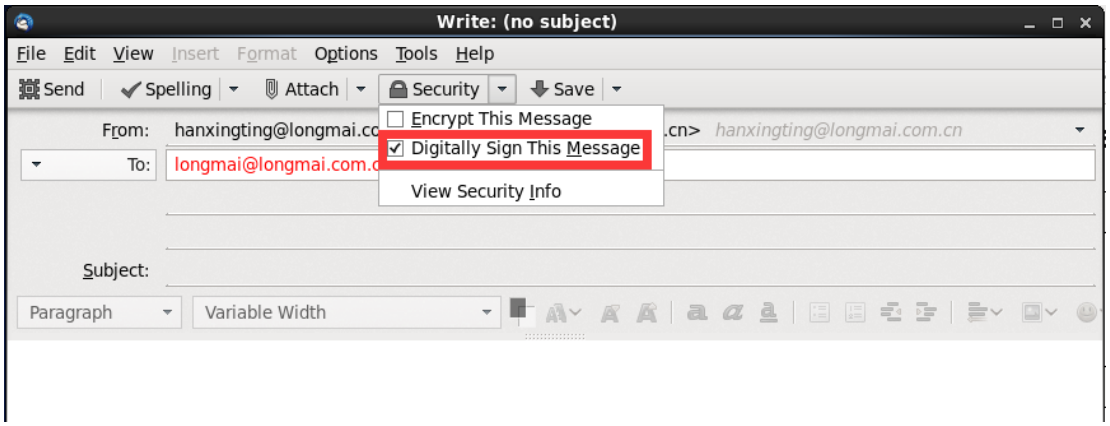
Now you can use the Email Account to sign and encrypt messages.

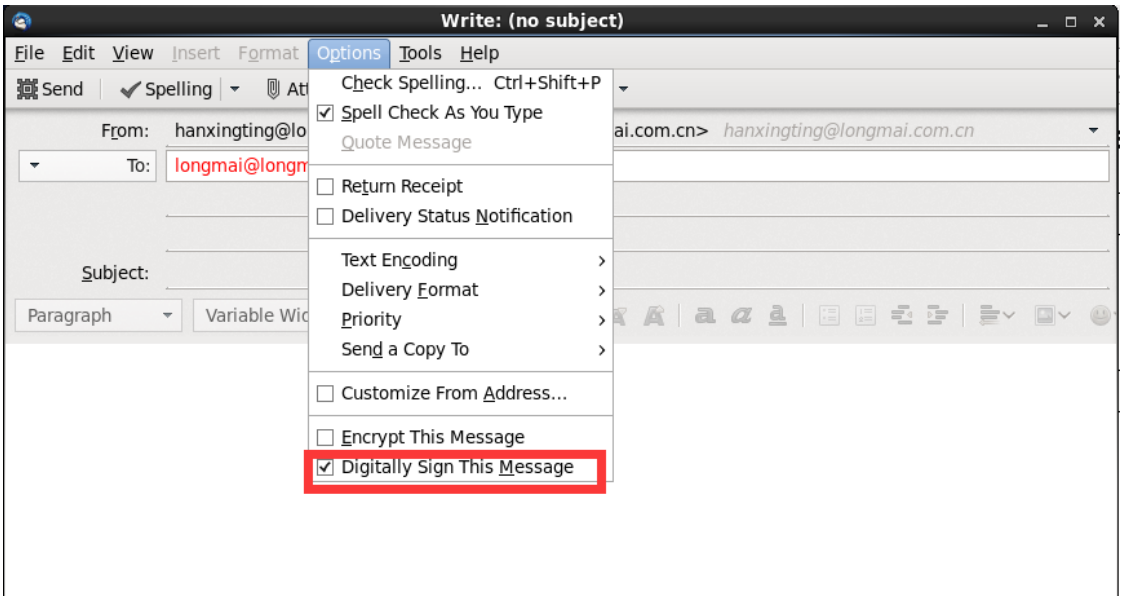
4.1.4 Using Thunderbird to send messages with Digital Signature

1. Start Thunderbird, click **New**. A new message editor will appear.



2. After the writing is done, click **Security** on the toolbar. Select **Digitally Sign This Message** from the drop-down list, or select **Options→Security →Digitally Sign This Message**.





3. Click **Send**. The PIN box will pop up if you never typed the PIN before. After typing the correct PIN, the email will be sent out.

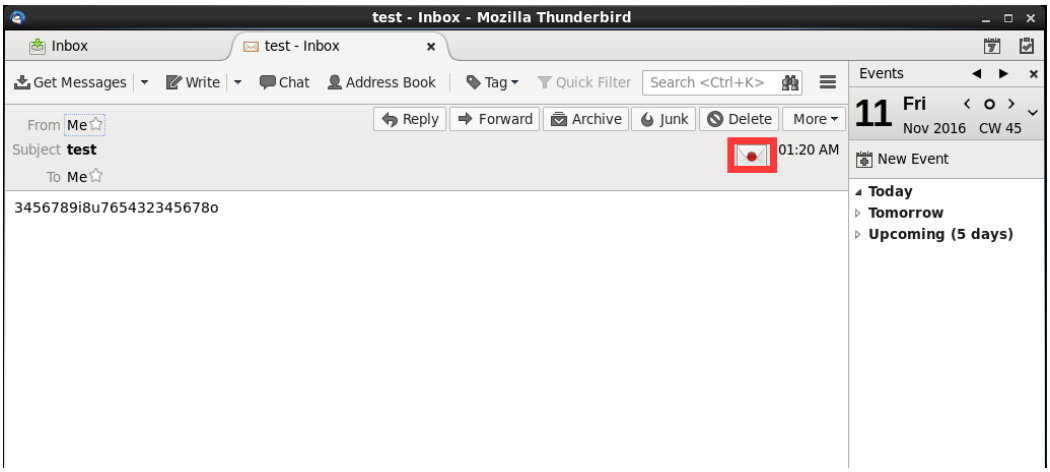
4.1.5 Obtaining Recipient's Public Key and Certificate

- To send an encrypted message, you must obtain the recipient's public key or certificate, then encrypt the message with the public key of the recipient (use the recipient's public key to encrypt). In this case, only the private key and corresponding public key, can be used to encrypted message and be received and read normally.
- To obtain the recipient's public key or certificate, ask the recipient to send a message with a digital signature and save the certificate when receiving

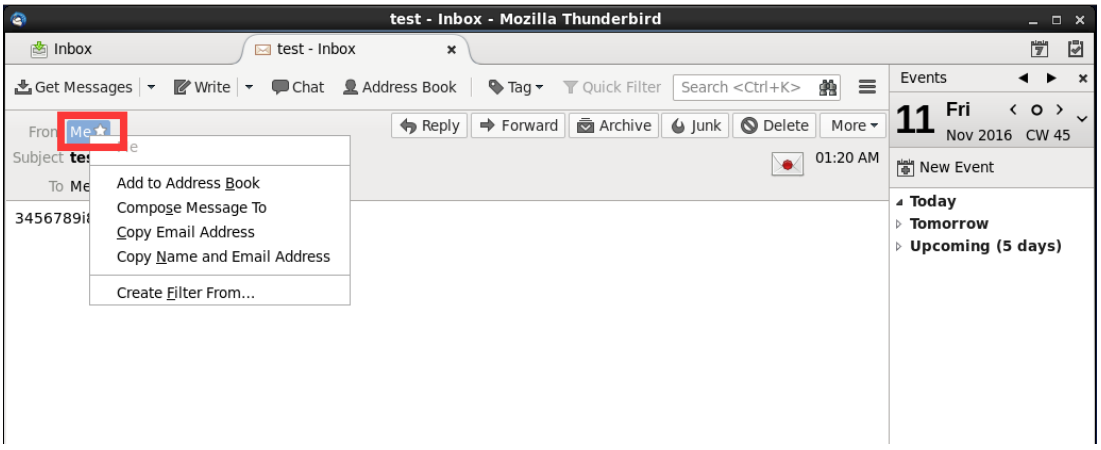
the message. In this way, you can obtain the opponent's public key and certificate.

To store the certificate or public key, follow the following steps:

1. Ask the recipient to send you a message with a digital signature, as described in the *previous section.*
2. Start Thunderbird to receive the message. Click the mail icon as marked below. A dialog box pops up, displaying the sender's information and signing certificate for you verification.



3. Click on the **From:** address as marked below.



4. Select **Edit Contact** from the pop-up menu to add the recipient's address to your address book. Thus, the recipient's certificate is associated with its address.

Actually, if you have ever received a message from the recipient, its address and certificate are associated automatically and recorded by Thunderbird. Later, if you want to send an encrypted message to the recipient, Thunderbird will use the associated certificate automatically when you enter the recipient's address in **To:** address.

4.1.6 Using Thunderbird to send Encrypted Messages

Make sure the recipient's public key or certificate have been obtained in the previous section when you sending an encrypted message.

To do so, perform the following operations:

- **Case 1: Direct response to the operations**

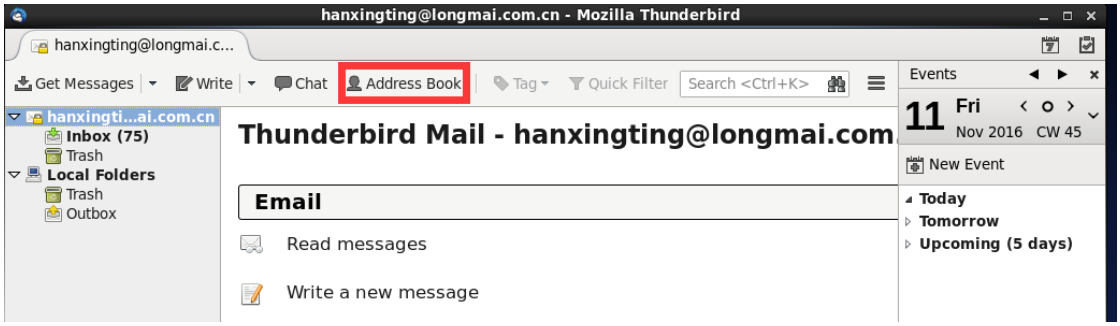
1. Start Thunderbird.
2. Open the message sent by the recipient and click **Reply** on the toolbar.
3. After the content of the message is complete, click **Security** →**Encrypt This Message**, or **Options** →**Encrypt This Message**.
4. Click **Send**, you will be asked for the PIN if you have not entered it before. Then click **OK**.

- **Case 2: Direct entry of the address of the recipient**

1. Start Thunderbird.
2. Click **New** to open a new message editor.
3. Type a correct address in the **To:** address, Thunderbird will use the certificate associated with the address as the encryption certificate automatically.
4. After the contents of the message is complete, click **Security** →**Encrypt This Message**, or **Options** →**Encrypt This Message**.
5. Click **Send**, you will be asked for the PIN if you have not entered it before. Then click **OK**.

- **Case 3: Selection of the recipient from Address book**

1. Start Thunderbird.
2. Select **Address Book**.



3. The Address Book is displayed as below.

4. Choose an address. Click **New**, a new message editor appears. The following operations are the same as in 1.4.3.

4.1.7 Using Thunderbird to send Signed, Encrypted messages

The operations are similar to those of sending an encrypted or signed message, except that you should select both **Encrypt This Message** and **Digitally Sign This Message** when configuring security.

5. About Century Longmai

Established in 2003, Century Longmai Technology Co., Ltd is one of the most leading information security device vendors in China with over 12 years' experience developing latest generation of digital security solutions and products for secure information access and transmission. Our product portfolios include PKI dongles, wireless PKI tokens, OTP tokens, smart card, smart card readers, electronic document protection solution, software license dongles, Smartcard readers and OEM services. Proved to be secure and convenient, our solutions and products are dedicated to help customers build safe, efficient and sustainable networks, financial systems and enjoy secure access to data and information everywhere whenever they want.

Century Longmai Technology Co., Ltd

3rd Floor, GongKong Building, No.1, WangZhuang Road, Haidian District, Beijing, China
Postcode: 100083
Tel: (86) 10-62323636 | Fax: (86) 10-62313636
Sales E-mail: info@longmai.net
Support E-mail: support@longmai.net
Website: http://www.longmai.net